ELSEVIER
Discrete Mathematics 254 (2002) 405–419
DISCRETE MATHEMATICS
www.elsevier.com/locate/disc

Galois theory for minors of finite functions

Nicholas Pippenger[1]

Department of Computer Science, The University of British Columbia, 2366 Main Mall, Vancouver, British Columbia, Canada V6T 1Z4

Received 21 March 2000; revised 19 March 2001; accepted 9 April 2001

Abstract

The motivating example for our work is given by sets of Boolean functions closed under taking minors. A Boolean function f is a *minor* of a Boolean function g if f is obtained from g by substituting an argument of f, the complement of an argument of f, or a Boolean constant for each argument of g. The theory of minors has been used to study threshold functions (also known as linearly separable functions) and their generalization to functions of bounded order (where the degree of the separating polynomial is bounded, but may be greater than one). We construct a Galois theory for sets of Boolean functions closed under taking minors, as well as for a number of generalizations of this situation. In this Galois theory we take as the dual objects certain pairs of relations that we call "constraints", and we explicitly determine the closure conditions on sets of constraints.

1. Introduction

The Galois theory of which we speak falls within the general framework described by Everett [6] and Ore [16], whereby an arbitrary binary relation between objects of two types gives rise to closure operations (in the sense of Ward [24]) on the sets of objects of each type, and to a one-to-one correspondence between the two types of closed sets. In such a theory one commonly starts with a given closure operation on sets of given primal objects, and seeks to discover dual objects, and a binary relation between primal and dual objects, so that the induced closure operation on the primary objects coincides with the given one. One also seeks an understanding of the induced closure operation on the dual objects, since it provides another avenue to understanding of the original closure operation.

The theory most similar to that which we seek is the Galois "polytheory" for finite functions constructed by Geiger [8] and independently by Bodnarchuk et al. [2]. Here the primal objects are finite functions (maps $f : \mathbf{B}_k^n \to \mathbf{B}_k$, where $\mathbf{B}_k = \{0, \ldots, k-1\}$

[1] The work reported here was supported by an NSERC Research Grant.

E-mail address: nicholas@cs.ubc.ca (N. Pippenger).

PII: S0012-365X(01)00297-7

and $n \geqslant 1$), and the closure operation is that in which the closed sets are "clones": sets of functions containing the monadic identity function and closed under adding dummy arguments, diagonalizing (or "identifying" arguments, which serves also for deleting dummy arguments), permuting arguments, and functional composition. Geiger and Bodnarchuk et al. established as dual objects finite relations called "invariants" (sets $R \subseteq \mathbf{B}_k^m$, where $m \geqslant 1$), and gave explicit descriptions of the appropriate binary relation between functions and invariants, and of the closure operation on invariants. This Galois polytheory can be seen as a development (for the case of finite functions and invariants) of the abstract Galois theory and Galois "endotheory" of Krasner (which had its inception [12] in the 1930s, prior to the work of Everett and Ore, and which is summarized in Krasner's posthumous papers [13,14]).

The motivating example for our work is given by sets of Boolean functions closed under taking minors: closed under adding dummy arguments, diagonalizing, permuting arguments, complementing arguments and substituting Boolean constants for arguments (see [22]). The best known example of such a set of functions is that of the "threshold" functions. The history of these is difficult to trace, but see [25] for many early references. Further examples are provided by the sets of Boolean functions of bounded order in the sense of Wang and Williams [23] (where the threshold functions constitute the special case of order at most one), and by the restrictions of these sets to monotone functions.

It will be natural, however, to generalize beyond the needs of these examples. Firstly, we generalize from Boolean functions (functions over $\mathbf{B}_2$) to "k-ean" functions (over $\mathbf{B}_k$). To do this we must adopt an appropriate generalization of the notion of "complement" that appears in the definition of "minor". We shall fix a set $\mathcal{Q}$ of monadic k-ean functions (maps $\sigma : \mathbf{B}_k \to \mathbf{B}_k$), and consider sets of functions closed under applying functions from $\mathcal{Q}$ to arguments. (This operation also subsumes that of substituting constants for arguments, by including constant functions in $\mathcal{Q}$.) Secondly, with functional composition out of the picture, there is no need to assume that the values of the functions are drawn from the same set as the arguments. Thus we consider "n-adic (k,l)-ean" functions (maps $f : \mathbf{B}_k^n \to \mathbf{B}_l$). We lose no generality by assuming that $\mathcal{Q}$ contains the identity function and is closed under composition, and thus that it is a monoid (or clone of monadic functions). Thus the general setting of our work will be one in which $\mathcal{Q}$ is a monadic k-ean clone, and we consider sets of (k,l)-ean functions that are closed under adding dummy arguments, diagonalization (identifying arguments), permuting arguments, and applying a function $\sigma \in \mathcal{Q}$ to an argument x_i of a function $f(x_1,\ldots,x_n)$ to yield the function $f(x_1,\ldots,x_{i-1},\sigma(x_i),x_{i+1},\ldots,x_n)$. We shall call such a set of functions *$\mathcal{Q}$-minor-closed*.

Many aspects of the theory we seek have been developed by Pöschel [17,18] (see also [19]). Pöschel's theory deals with functions whose several arguments may be of different "sorts", and whose values may belong to yet another sort. (The sorts are finite domains, corresponding to "types" in a programming language.) By choosing all the argument sorts to be one domain comprising k elements and the value sort to be another domain comprising l elements, our Theorems 2.1 and 3.2 correspond to cases of Satz 6.1.6 of [19]. We have not followed this path, but have chosen different dual objects, which we call "constraints". These constraints satisfy somewhat different closure conditions than Pöschel's invariants, they give a very direct reformulation of the Boolean equations used by Ekin et al. [5], and they have led to a further generalization due to Hellerstein [11].

The plan of our work is as follows. In Section 2 we shall start by "turning off" the minor-closure operations insofar as possible. Thus we shall construct the Galois theory for $\mathscr{I}$-minor-closed sets, where $\mathscr{I}$ is the monadic clone that contains only the identity function on k elements. Such a theory of "identification minors" for Boolean functions has been constructed by Ekin et al. [5], taking "Boolean equations" as the dual objects. That paper also gives many examples of sets of Boolean functions closed under taking identification minors, together with their characterizations by Boolean equations. Instead of equations, we shall use pairs of relations that we call "constraints" as the dual objects. This choice will facilitate the coming generalization to other minor-closure operations, and reveals the Galois polytheory as the special case in which the two relations of a constraint coincide to form an invariant. Of course in the Boolean case our theory is equivalent to that of Ekin et al. (as we shall show explicitly in the appendix), but even in this case we go further and determine the closed sets of dual objects.

In Section 3 we consider the general case of $\mathscr{Q}$-minor-closed sets of (k,l)-ean functions. Since we are now considering sets closed under more operations than in Section 2, the constraints that we introduced there will still be sufficient as dual objects, but some of them will no longer be necessary, and the closure operation on the sets of surviving constraints will be stronger. We conclude Section 3 with some miscellaneous observations on $\mathscr{Q}$-minor-closed sets of functions.

2. Identification minors

An *n-adic* (k,l)*-ean function* is a map $f:\mathbf{B}_k^n \to \mathbf{B}_l$. A (k,k)-ean function will be called simply a *k-ean function*. We shall say that an m-adic function g is a *minor* of a f if there exists a map $h:\{1,\ldots,n\}\to\{1,\ldots,m\}$ such that $g(x_1,\ldots,x_m)=f(x_{h(1)},\ldots,x_{h(n)})$. If $m=n$ and h is a bijection, we shall speak of *permutation* of arguments. If h is not injective, we shall speak of *diagonalization* or *identification* of arguments. If h is not surjective, we shall speak of adding *dummy* arguments. A set $\mathscr{F}$ of functions is *minor-closed* if $g\in\mathscr{F}$ whenever g is a minor of f and $f\in\mathscr{F}$.

An *m-ary k-ean relation* is a set $R\subseteq\mathbf{B}_k^m$, which we shall regard as a set of *columns* comprising m elements from $\mathbf{B}_k$. An *m-ary* (k,l)*-ean constraint* is a pair (R,S), where R is an m-ary k-ean relation called the *antecedent*, and S is an m-ary l-ean relation called the *consequent*.

If $M\in\mathbf{B}_k^{m\times n}$ is an $m\times n$ matrix of elements from $\mathbf{B}_k$ and R is an m-ary k-ean relation, we shall write $M\prec R$ to mean that every column of M belongs to R. If furthermore f is an n-adic (k,l)-ean function, we shall write $f(M)$ for the column of elements from $\mathbf{B}_l$ obtained by applying f to each row of M.

If f is an n-adic (k,l)-ean function and (R,S) is an m-ary (k,l)-ean constraint, we shall say that f *satisfies* (R,S) (written $f \approx (R,S)$) if, for every $m \times n$ matrix M such that $M \prec R$, we have $f(M) \in S$. This notion of a function satisfying a constraint is the cornerstone of this paper, and will give rise to the Galois correspondence that we seek.

As an example, if $R = \{\binom{0}{0}, \binom{0}{1}, \binom{1}{1}\}$, then the constraint (R,R) is satisfied by the Boolean functions that are "monotone" or "non-decreasing"; that is, the $f : \mathbf{B}_2^n \to \mathbf{B}_2$ such that $x_1 \leqslant y_1, \ldots, x_n \leqslant y_n$ imply $f(x_1,\ldots,x_n) \leqslant f(y_1,\ldots,y_n)$. This set of functions is closed under composition as well as taking minors, and is characterized in the theory of Geiger and Bodnarchuk et al. by the invariant R. If $S = \{\binom{0}{0}, \binom{1}{0}, \binom{1}{1}\}$, then the constraint (R,S) is satisfied by the Boolean functions that are "non-increasing"; that is, the $f : \mathbf{B}_2^n \to \mathbf{B}_2$ such that $x_1 \leqslant y_1, \ldots, x_n \leqslant y_n$ imply $f(x_1,\ldots,x_n) \geqslant f(y_1,\ldots,y_n)$. This set of functions is not closed under composition, and it cannot be characterized by invariants, but it can be characterized by constraints.

If (R,S) is a constraint, then the set of functions satisfying (R,S) is minor-closed. Furthermore, if $\mathscr{T}$ is any set of constraints, the set of functions satisfying all the constraints in $\mathscr{T}$ is an intersection of minor-closed sets, and is therefore itself a minor-closed set. Thus the sets of functions that are characterized by the constraints that they satisfy are all minor-closed. The following theorem shows that every minor-closed set of functions is characterized by the constraints that are satisfied by its functions.

Theorem 2.1. *Let $\mathscr{F}$ be a minor-closed set of functions and let g be any function not belonging to $\mathscr{F}$. Then there is a constraint (R,S) that is satisfied by every function in $\mathscr{F}$ but that is not satisfied by g.*

Proof. Suppose that g is n-adic. Let $\mathscr{F}_n$ be the set of n-adic functions in $\mathscr{F}$. Let M be a $k^n \times n$ matrix whose rows are all the n-tuples of elements from $\mathbf{B}_k$, let R be the k^n-ary relation comprising the columns of M, and let S be the k^n-ary relation comprising the columns $f(M)$, where f runs through $\mathscr{F}_n$.

Firstly, we claim that every function in $\mathscr{F}$ satisfies the constraint (R,S). To see this, suppose that f' is an n'-adic function from $\mathscr{F}$, and that M' is a $k^n \times n'$ matrix of elements from $\mathbf{B}_k$ such that $M' \prec R$. We must show that $f'(M')$ belongs to S. Since $M' \prec R$, each of the n' columns of M' must equal one of the n columns of M. Define the map $h : \{1,\ldots,n'\} \to \{1,\ldots,n\}$ so that column i of M' equals column $h(i)$ of M. The n-adic function f defined by $f(x_1,\ldots,x_n) = f'(x_{h(1)},\ldots,x_{h(n')})$ is a minor of f', and therefore belongs to $\mathscr{F}_n$. We have $f'(M') = f(M)$. Since $f(M)$ belongs to S, the proof of the claim is complete.

Secondly, we claim that g does not satisfy (R,S). Suppose, to obtain a contradiction, that g does satisfy (R,S), so that in particular $g(M)$ belongs to S. Then there is a function f in $\mathscr{F}_n$ such that $f(M) = g(M)$. But this implies that $f = g$, since every n-tuple of elements from $\mathbf{B}_k$ appears as a row of M. This contradicts the hypothesis that g does not belong to $\mathscr{F}$, and completes the proof of the second claim. $\square$

At this point we have an analog, in terms of constraints, of the main result that Ekin et al. obtain in terms of Boolean equations. That these results are essentially equivalent is established in the appendix, where we show that for every Boolean constraint, there is a Boolean equation of a certain type that is satisfied by exactly the same functions, and vice versa.

Our next goal is to determine the closure operation on the constraints that is induced by this Galois correspondence. Thus we seek to answer the question: when can a set of constraints be characterized by the functions that satisfy them? To do this we need to consider various operations on constraints.

We shall refer to a constraint (R, S) in which a column belongs to R or S if and only if all its arguments are equal as an *equality* constraint. We shall refer to a constraint of the form $(\mathbf{B}_k^m, \mathbf{B}_l^m)$, with all possible columns in both antecedent and consequent, as a *trivial* constraint. We shall refer to a constraint of the form $(\emptyset, \emptyset)$ as an *empty* constraint.

We refer to the row positions of a relation or constraint as "arguments" (in the same way that we refer to the column positions of functions as arguments). We shall say that a constraint (R, S) is a *simple minor* of a constraint (R', S') if there is a natural number $0 \leqslant p \leqslant n$ and a map $h : \{1, \ldots, n\} \to \{1, \ldots, m + p\}$ such that

$$R \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \exists x_{m+1} \cdots \exists x_{m+p}\ R' \begin{pmatrix} x_{h(1)} \\ \vdots \\ x_{h(n)} \end{pmatrix}$$

and

$$S \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \exists x_{m+1} \cdots \exists x_{m+p}\ S' \begin{pmatrix} x_{h(1)} \\ \vdots \\ x_{h(n)} \end{pmatrix}.$$

If $m = n$, $p = 0$ and h is a bijection, we shall speak of *permutation* of arguments. If h maps several elements of $\{1, \ldots, n\}$ to the same element of $\{1, \ldots, m\}$, we shall speak of *diagonalization* or *identification* of arguments. If h maps elements of $\{1, \ldots, n\}$ to an element of $\{m+1, \ldots, m+p\}$, we shall speak of *projection* or *existential quantification* of arguments. If h is not surjective, we shall speak of adding *dummy* arguments.

We shall say that a constraint (R, S) is obtained from a constraint (R', S) by *restricting the antecedent* if $R \subseteq R'$. We shall say that a constraint (R, S) is obtained from a constraint (R, S') by *extending the consequent* if $S \supseteq S'$. We shall say that the constraint $(R, S \cap S')$ is obtained from the constraints (R, S) and (R, S') by *intersecting consequents*.

We shall say that a set of constraints is *minor-closed* if it contains the binary equality constraint, contains the unary empty constraint and is closed under taking simple minors, restricting antecedents, extending consequents and intersecting consequents. We shall show that the minor-closed sets of constraints are exactly the sets of constraints that are characterized by the functions that satisfy them.

If f is a function, then the set of constraints satisfied by f is minor-closed. Furthermore, if $\mathscr{F}$ is any set of functions, the set of constraints satisfied by all the functions in $\mathscr{F}$ is an intersection of minor-closed sets, and is therefore itself minor-closed. Thus the sets of constraints that are characterized by the functions that satisfy them are all minor-closed. The following theorem shows that every minor-closed set of constraints is characterized by the set of functions that satisfies all of its constraints.

Theorem 2.2. *Let $\mathscr{T}$ be a minor-closed set of constraints, and let (R,S) be a constraint not belonging to $\mathscr{T}$. Then there exists a function f that satisfies every constraint in $\mathscr{T}$ but that does not satisfy (R,S).*

To prove Theorem 2.2, we shall follow the strategy used by Geiger [8]. First we shall introduce the usual notion of a partial function, and define what it means for a partial function to satisfy a constraint in a way that yields the following restriction principle: if a function f satisfies a constraint, then any restriction of f also satisfies that constraint. We then prove an analogue of Theorem 2.2 in which "function" is weakened to "partial function". Finally, we show that if a partial function g satisfies all the constraints in some minor-closed set $\mathscr{T}$ of constraints, then there exists some extension of g to a total function f that also satisfies all the constraints in $\mathscr{T}$.

Before proceeding, we observe that minor-closed sets of constraints are also closed under two other operations.

Lemma 2.3. *A minor-closed set of constraints is also closed under taking intersections (that is, obtaining $(R \cap R', S \cap S')$ from (R,S) and (R',S')), and taking products (that is, obtaining $(R \times R', S \times S')$ from (R,S) and (R',S')).*

Proof. From (R,S) we can obtain $(R \cap R', S)$ by restricting the antecedent, and from (R',S') we can obtain $(R \cap R', S')$ in the same way. Then we can obtain $(R \cap R', S \cap S')$ from $(R \cap R', S)$ and $(R \cap R', S')$ by intersecting consequents. Thus a minor-closed set of constraints is also closed under taking intersections.

Suppose that (R,S) and (R',S') are m-ary and m'-ary constraints, respectively. By adding m' dummy arguments to (R,S), we can obtain a constraint (R^*,S^*) in which the m arguments of (R,S) are followed by m' dummy arguments. Similarly, by adding m dummy arguments to (R',S'), we can obtain a constraint (R'^*,S'^*) in which the m' arguments of (R',S') follow m dummy arguments. Then we can obtain $(R \times R', S \times S')$ by intersecting (R^*,S^*) and (R'^*,S'^*). Thus a minor-closed set of constraints is also closed under taking products. □

An n-adic (k,l)-ean *partial function* g consists of a subset $D \subseteq \mathbf{B}_k^n$ called the *domain* of g and a map $g : D \to \mathbf{B}_l$. Thus a function, which for emphasis we may refer to as a *total function*, is simply a partial function whose domain is all of $\mathbf{B}_k^n$. If the domain D of a partial function g is a subset of the domain of the partial function f, and if $g(x) = f(x)$ for every n-tuple in D, we shall say that g is a *restriction* of f, and that f is an *extension* of g.

If g is an n-adic (k,l)-ean partial function and (R,S) is an m-ary (k,l)-ean constraint, we shall say that g *satisfies* (R,S) if, for every $m\times n$ matrix M such that $M \prec R$, and such that every row of M belongs to the domain of g, we have $g(M)\in S$. This definition yields the restriction principle stated above: if a partial function f satisfies a constraint, so does every restriction of f.

Lemma 2.4. *A minor-closed set of constraints contains all trivial constraints and all equality constraints.*

Proof. By projecting one of the arguments of the binary equality constraint, we obtain the unary trivial constraint, and by then adding $m-1$ dummy arguments, we obtain the m-ary trivial constraint.

By adding $m-2$ dummy arguments to the binary equality constraint, we obtain an m-ary constraint (R,S) in which a column belongs to R or S if and only if a particular pair of consecutive arguments are equal. By intersecting $m-1$ such constraints (for the $m-1$ pairs of consecutive arguments), we obtain the m-ary equality constraint. □

Proposition 2.5. *Let $\mathscr{T}$ be a minor-closed set of constraints, and let (R,S) be a constraint not belonging to $\mathscr{T}$. Then there exists a partial function g that satisfies every constraint in $\mathscr{T}$ but that does not satisfy (R,S).*

Proof. Suppose that (R,S) is m-ary. The relation S cannot contain all l^m m-tuples of elements from $\mathbf{B}_l$, for if it did, then (R,S) could be obtained from a trivial constraint by restricting the antecedent, and thus would belong to the minor-closed set $\mathscr{T}$. The minor-closed set $\mathscr{T}$ cannot contain $(R,\mathbf{B}_l^m\backslash\{s\})$ for every s that does not belong to S, for if it did, then by intersection of consequents it would also contain their intersection (R,S). Fix some m-tuple s that does not belong to S and for which $(R,\mathbf{B}_l^m\backslash\{s\})$ does not belong to $\mathscr{T}$.

Suppose that the relation R contains n m-tuples. Define an $m\times n$ matrix M whose columns are the columns of R in some fixed order. Define a partial function g by taking the domain of g to be the set of rows of M, with the values of g given by $g(M)=s$.

Firstly, we claim that g satisfies every constraint in $\mathscr{T}$. Suppose, to obtain a contradiction, that (R',S') is an m'-ary constraint in $\mathscr{T}$ that is not satisfied by g. Let M' be an $m'\times n$ matrix such that $M'\prec R'$ and $g(M')=s'\notin S'$. Every row of M' must belong to the domain of g, and must therefore also be a row of M. Define the map $h:\{1,\dots,m'\}\to\{1,\dots,m\}$ such that row i of M' equals row $h(i)$ of M. We shall also use h to denote the maps $h:\mathbf{B}_k^m\to\mathbf{B}_k^{m'}$ and $h:\mathbf{B}_l^m\to\mathbf{B}_l^{m'}$ defined by

$$h\left(\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}\right)=\begin{pmatrix} x_{h(1)} \\ \vdots \\ x_{h(m')} \end{pmatrix}.$$

Finally, we shall define the m-ary relation $h^{-1}(R')$ by $x \in h^{-1}(R')$ if and only if $h(x) \in R'$, the m-ary relation $h^{-1}(S')$ by $x \in h^{-1}(S')$ if and only if $h(x) \in S'$, and the m-ary constraint $h^{-1}((R', S')) = (h^{-1}(R'), h^{-1}(S'))$. The constraint $h^{-1}((R', S'))$ is a minor of (R', S'), and thus belongs to $\mathscr{T}$.

If r belongs to R, then r appears as a column of M, and the corresponding column r' of M' belongs to R'. Since $h(r) = r' \in R'$, we have $r \in h^{-1}(R')$. Thus $R \subseteq h^{-1}(R')$. Since every entry of s or s' is obtained by applying g to the corresponding row of M or M', we have $h(s) = s'$. Since $h(s) = s'$ does not belong to S', s does not belong to $h^{-1}(S')$. Thus $\mathbf{B}_l^m \backslash \{s\} \supseteq h^{-1}(S')$. Since $\mathscr{T}$ contains $h^{-1}((R', S'))$, it also contains the constraint $(R, \mathbf{B}_l^m \backslash \{s\})$ obtained from it by restricting the antecedent and extending the consequent. This contradicts the choice of s, and completes the proof of the first claim.

Secondly, we claim that g does not satisfy (R, S). For if it did, then since $M \prec R$, we would have that $s = g(M)$ belongs to S, again contradicting the choice of s. This completes the proof of the second claim. □

Proposition 2.6. *Let $\mathscr{T}$ be a minor-closed set of constraints. If g is a partial function satisfying all the constraints in $\mathscr{T}$, then there is an extension of g to a total function that also satisfies all the constraints in $\mathscr{T}$.*

Proof. Suppose that g is n-adic. If g is not itself a total function, let y be some n-tuple of elements from $\mathbf{B}_k$ that does not belong to the domain D of g. We claim that there exists a value $c \in \mathbf{B}_l$ such that the extension g_c with domain $D \cup \{y\}$ and values given by

$$g_c(x) = \begin{cases} c & \text{if } x = y, \\ g(x) & \text{otherwise.} \end{cases}$$

also satisfies all the constraints in $\mathscr{T}$. Repetition of this process yields a total extension of g that satisfies all the constraints in $\mathscr{T}$.

Suppose, to obtain a contradiction, that for every value $c \in \mathbf{B}_l$, there is a constraint (R_c, S_c) in $\mathscr{T}$ such that g_c does not satisfy (R_c, S_c), and thus that there is an $M_c \prec R_c$ such that every row of M_c belongs to $D \cup \{y\}$ and $g_c(M_c) \notin S_c$. We may assume that (R_c, S_c) has the smallest possible number of arguments, and M_c the smallest possible number of rows. The n-tuple y must appear at least once as a row in every M_c, for if not we would have $g_c(M_c) = g(M_c)$, and the assumption that g satisfies $(R_c, S_c) \in \mathscr{T}$ would imply that g_c satisfies (R_c, S_c), a contradiction. Furthermore, y must appear exactly once as a row in M_c, for if not we could, by deleting all but one such row from M_c and diagonalizing the corresponding arguments of (R_c, S_c), obtain a constraint in $\mathscr{T}$ with fewer rows and still not satisfied by g_c. We shall call the row in which y appears as a row of M_c the *critical* row of M_c.

Since the minor-closed set $\mathscr{T}$ contains each (R_c, S_c), it also contains their product (R, S), where $R = R_0 \times \cdots \times R_{l-1}$ and $S = S_0 \times \cdots \times S_{l-1}$. We then have $M \prec (R, S)$, where the matrix M is obtained by vertically concatenating the matrices $M_0, \ldots, M_{l-1}$.

In (R,S) and M, we shall refer to the rows arising from (R_c,S_c) and M_c as *c-rows*, and to the row corresponding to the critical row in (R_c,S_c) and M_c as the *c-critical* row in (R,S) and M.

By adding dummy arguments to an l-ary equality constraint, we can obtain a constraint (R',S') in $\mathscr{T}$, having the same number of arguments as (R,S), in which a column belongs to R' or S' if and only if all l critical arguments are equal. Since $\mathscr{T}$ contains both (R,S) and (R',S'), it also contains their intersection $(\hat{R},\hat{S})=(R\cap R',S\cap S')$.

Say a column of S_c is *c-consistent* if its non-critical entries agree with the corresponding entry of $g_c(M_c)$. A c-consistent column cannot contain the value c in its critical row, else we would have $g_c(M_c)\in S_c$, a contradiction.

Say a column of S is *consistent* if, for every $c\in \mathbf{B}_l$, the column comprising the entries in the c-rows is c-consistent. A consistent column of S cannot have the value c in its c-critical row, and thus cannot have any single value in all l of its critical rows. It follows that $\hat{S}=S\cap S'$ does not contain any c-consistent columns.

Since $\mathscr{T}$ contains $(\hat{R},\hat{S})$, it also contains the constraint $(\tilde{R},\tilde{S})$ obtained from $(\hat{R},\hat{S})$ by projecting the l critical arguments. Since $\hat{S}$ does not contain any c-consistent columns, neither does $\tilde{S}$. Let $\tilde{M}$ denote the matrix obtained from M by deleting the l critical rows (which are the rows equal to y). Then $\tilde{M}\prec\tilde{R}$. Furthermore, all rows of $\tilde{M}$ belong to D. Since $\tilde{S}$ does not contain any c-consistent columns, $g(\tilde{M})\notin\tilde{S}$, so g does not satisfy the constraint $(\tilde{R},\tilde{S})$ in $\mathscr{T}$. This contradiction completes the proof of the proposition. □

Proof of Theorem 2.2. Given a minor-closed set $\mathscr{T}$ of constraints and a constraint $(R,S)\notin\mathscr{T}$, Proposition 2.5 yields a partial function g that satisfies every constraint in $\mathscr{T}$ but that does not satisfy (R,S). By Proposition 2.6, there is an extension of g to a total function f that also satisfies every constraint in $\mathscr{T}$. By the restriction principle, f does not satisfy (R,S), since its restriction g does not satisfy (R,S). □

3. General minors

Let $\mathscr{Q}$ be a set of monadic k-ean functions that contains the identity function and is closed under composition. We shall let $\mathscr{I}$ denote the set containing just the identity function, and $\mathscr{U}$ the set containing all monadic k-ean functions.

We shall say that an m-adic function g is a *$\mathscr{Q}$-minor* of an n-adic function f if there exists a map $h:\{1,\ldots,n\}\to\{1,\ldots,m\}$ and functions $\sigma_1,\ldots,\sigma_n\in\mathscr{Q}$ such that $f(x_1,\ldots,x_m)=f(\sigma_1(x_{h(1)}),\ldots,\sigma_n(x_{h(n)}))$. A set $\mathscr{F}$ of functions is *$\mathscr{Q}$-minor-closed* if $g\in\mathscr{F}$ whenever g is a minor of f and $f\in\mathscr{F}$. Thus the $\mathscr{I}$-minor-closed sets of functions are just the sets that are minor-closed in the sense of the preceding section.

If x is a column of elements from $\mathbf{B}_k$ and σ is a function from $\mathscr{Q}$, we shall write $\sigma(x)$ for the column obtained from x by applying σ to each entry of x. If R is a k-ean relation, we shall write $\mathrm{sat}_{\mathscr{Q}}(R)$ for the relation comprising all the columns obtained by applying a function from $\mathscr{Q}$ to a column from R. The operation $\mathrm{sat}_{\mathscr{Q}}$ is a closure operation: it is inflationary ($\mathrm{sat}_{\mathscr{Q}}(R) \supseteq R$), increasing ($\mathrm{sat}_{\mathscr{Q}}(R) \subseteq \mathrm{sat}_{\mathscr{Q}}(R')$ if $R \subseteq R'$) and idempotent ($\mathrm{sat}_{\mathscr{Q}}(\mathrm{sat}_{\mathscr{Q}}(R)) = \mathrm{sat}_{\mathscr{Q}}(R)$). We shall say that a relation R is *$\mathscr{Q}$-saturated* if $\mathrm{sat}_{\mathscr{Q}}(R) = R$, and that a constraint (R,S) is *$\mathscr{Q}$-saturated* if its antecedent R is $\mathscr{Q}$-saturated.

If (R,S) is a $\mathscr{Q}$-saturated constraint, then the set of functions satisfying (R,S) is $\mathscr{Q}$-minor-closed. Furthermore, if $\mathscr{T}$ is any set of $\mathscr{Q}$-saturated constraints, the set of functions satisfying all the constraints in $\mathscr{T}$ is an intersection of $\mathscr{Q}$-minor-closed sets, and is therefore itself a $\mathscr{Q}$-minor-closed set. Thus the sets of functions that are characterized by the $\mathscr{Q}$-saturated constraints that they satisfy are all $\mathscr{Q}$-minor-closed. Our next goal is Theorem 3.2, which shows that every $\mathscr{Q}$-minor-closed set of functions is characterized by the $\mathscr{Q}$-saturated constraints that are satisfied by its functions.

Proposition 3.1. *Let $\mathscr{F}$ be a $\mathscr{Q}$-minor-closed set of functions. If every function in $\mathscr{F}$ satisfies the constraint (R,S), then every function in $\mathscr{F}$ also satisfies the $\mathscr{Q}$-saturated constraint* $(\mathrm{sat}_{\mathscr{Q}}(R), S)$.

Proof. Suppose that (R,S) and $(\mathrm{sat}_{\mathscr{Q}}(R), S)$ are m-ary. Let f be an n-adic function in $\mathscr{F}$ and let M be an $m \times n$ matrix such that $M \prec \mathrm{sat}_{\mathscr{Q}}(R)$. We must show that $f(M)$ belongs to S.

Since $M \prec \mathrm{sat}_{\mathscr{Q}}(R)$, there is an $m \times n$ matrix M' such that $M' \prec R$ and, for every i in $\{1,\dots,n\}$, column i of M is obtained by applying some function σ_i in $\mathscr{Q}$ to column i of M'. The n-adic function f' defined by

$$f'(x_1,\dots,x_n) = f(\sigma_1(x_1),\dots,\sigma_n(x_n))$$

is a $\mathscr{Q}$-minor of f, and therefore also belongs to $\mathscr{F}$. Thus f' satisfies (R,S), so that $f'(M')$ belongs to S. But $f(M) = f'(M')$, so that $f(M)$ also belongs to S. $\square$

Theorem 3.2. *Let $\mathscr{F}$ be a $\mathscr{Q}$-minor-closed set of functions and let g be any function not belonging to $\mathscr{F}$. Then there is a $\mathscr{Q}$-saturated constraint that is satisfied by every function in $\mathscr{F}$, but that is not satisfied by g.*

Proof. Since $\mathscr{I} \subseteq \mathscr{Q}$, $\mathscr{F}$ is $\mathscr{I}$-minor-closed, and thus by Theorem 2.1 there exists a constraint (R,S) that is satisfied by every function in $\mathscr{F}$, but that is not satisfied by g. By Proposition 3.1 the $\mathscr{Q}$-saturated constraint $(\mathrm{sat}_{\mathscr{Q}}(R), S)$ is also satisfied by every function in $\mathscr{F}$, but (since (R,S) is obtained from it by restricting the antecedent) it is not satisfied by g. $\square$

This theorem shows that, when considering $\mathscr{Q}$-minor-closed sets of functions, we may restrict attention to $\mathscr{Q}$-saturated constraints as the dual objects. Our next goal is to determine the closure operation induced on these dual objects.

Say that a set of constraints (not necessarily all $\mathscr{Q}$-saturated) is *$\mathscr{Q}$-minor-saturated* if it is minor-closed (in the sense of the preceding section) and if it contains the constraint (R',S) whenever it contains the constraint (R,S) and $\mathrm{sat}_{\mathscr{Q}}(R') = \mathrm{sat}_{\mathscr{Q}}(R)$. The set of constraints satisfied by every function in a $\mathcal{Q}$-minor-closed set of functions is $\mathcal{Q}$-minor saturated, for by the remarks preceding Theorem 2.2 it is minor-closed (in the sense of the preceding section), and if it contains a constraint (R, S), then by Proposition 3.1 it also contains the constraint $(\mathrm{sat}_{\mathcal{Q}}(R), S)$, and thus (being minor-closed) it also contains all the constraints (R', S) such that $\mathrm{sat}_{\mathcal{Q}}(R') = \mathrm{sat}_{\mathcal{Q}}(R)$, since these are obtained from $(\mathrm{sat}_{\mathcal{Q}}(R), S)$ by restricting the antecedent.

Say that a set of $\mathcal{Q}$-saturated constraints is *$\mathcal{Q}$-minor-closed* if it is the set of the $\mathcal{Q}$-saturated constraints belonging to some $\mathcal{Q}$-minor-saturated set of constraints. The $\mathcal{Q}$-minor-closed sets of $\mathcal{Q}$-saturated constraints are the closed sets of dual objects, when the latter are taken to be the $\mathcal{Q}$-saturated constraints.

Theorem 3.3. *A set of $\mathcal{Q}$-saturated constraints is $\mathcal{Q}$-minor-closed if and only if it contains the binary equality constraint and is closed under taking simple minors, restricting antecedents to $\mathcal{Q}$-saturated relations, extending consequents and intersecting consequents.*

Proof. (*if*). Let $\mathcal{T}$ be a set of $\mathcal{Q}$-saturated constraints that contains the binary equality constraint and is closed under taking simple minors, restricting antecedents to $\mathcal{Q}$-saturated relations, extending consequents and intersecting consequents. Let $\mathcal{T}'$ be the smallest $\mathcal{Q}$-minor-saturated set of constraints that includes $\mathcal{T}$. The only constraints in $\mathcal{T}'$ that are not also in $\mathcal{T}$ are those obtained from constraints in $\mathcal{T}$ by restricting the antecedent to a relation that is not $\mathcal{Q}$-saturated. Thus $\mathcal{T}$ is the set of the $\mathcal{Q}$-saturated constraints in the $\mathcal{Q}$-minor-saturated set $\mathcal{T}'$ of constraints.

(*only if*). The binary equality constraint is $\mathcal{Q}$-saturated, and the operations of taking simple minors, restricting antecedents to $\mathcal{Q}$-saturated relations, extending consequents and intersecting consequents all yield $\mathcal{Q}$-saturated constraints when applied to $\mathcal{Q}$-saturated constraints. Since a $\mathcal{Q}$-minor-saturated set of constraints contains the binary equality constraint and is closed under these operations, so is the set of the $\mathcal{Q}$-saturated constraints that it contains. $\square$

The classification of finite functions into $\mathcal{Q}$-minor-closed sets is in general much finer than that into clones (even in the case $\mathcal{Q} = \mathcal{U}$, which gives the coarsest classification). One manifestation of this phenomenon is that, while there are only countably many Boolean clones (see [20]), there are uncountably many Boolean $\mathcal{U}$-minor-closed sets, as will be shown with the aid of the following proposition.

Proposition 3.4. *For $n \geqslant 4$, define the n-adic Boolean function f_n by*

$$f_n(x_1, \ldots, x_n) = \begin{cases} 1 & \text{if } \#\{i\colon x_i = 1\} \in \{1, n-1\}, \\ 0 & \text{otherwise.} \end{cases}$$

Then if $m \neq n$, f_m is not a $\mathcal{U}$-minor of f_n.

Proof. If $m > n$, the conclusion is immediate, since a $\mathscr{U}$-minor of any function f depends essentially on at most as many arguments as f. So suppose that $m<n$.

The proof depends on two observations. First, if we fix at most three arguments of f_m to constant values, the resulting function of the remaining arguments is *not* a constant function. Secondly, if we fix at least two arguments of f_n to 0s, and at least two arguments to 1s, the resulting function of the remaining arguments *is* a constant function (always assuming the value 0).

Suppose, to obtain a contradiction, that f_m is a $\mathscr{U}$-minor of f_n, so that every argument of f_n is an argument of f_m, the complement of an argument of f_m, or a constant (that is, so that $f_m(x_1,\ldots,x_m) = f_n(\sigma(x_{h(1)}),\ldots,\sigma_n(x_{h(n)}))$, where $h: \{1,\ldots,n\} \to \{1,\ldots,m\}$ and $\sigma_1,\ldots,\sigma_n : \mathbf{B}_2 \to \mathbf{B}_2$). Furthermore, every argument of f_m must appear at least once as an argument of f_n, since f_m depends on all its arguments.

Suppose first that every argument of f_m appears, either directly or complemented, exactly once as an argument of f_n. Then, since $m < n$, at least one argument of f_n must be a constant, say c. Set one argument of f_m if direct to c, and if complemented to the complementary value $\bar{c}$, and set two other arguments of f_n if direct to $\bar{c}$ and if complemented to c. Since we have set just three arguments of f_m to constants, the resulting function of the remaining arguments of f_m is not a constant function. But since we have thereby set two arguments of f_n to 0s and two to 1s, the resulting function is the constant function with value 0, a contradiction.

Suppose then that some argument of f_m appears, either directly or complemented or both, at least twice as an argument of f_n. Set some such argument of f_m to 0. This will result in setting at least two arguments of f_n to constants, either two to 0s, two to 1s, or one to each of 0 and 1. In any case, by setting two other arguments of f_m to appropriately chosen constants, we can set two further arguments of f_n so that at least two are set to 0s and at least two are set to 1. Since we have done this by setting just three arguments of f_m to constants, we again obtain a contradiction. This completes the proof that f_m is not a $\mathscr{U}$-minor of f_n for $m < n$. $\square$

From Proposition 3.4, we see that every subset of $\{f_4, f_5, \ldots, f_n, \ldots\}$ generates a different $\mathscr{U}$-minor-closed set of functions, and thus that there are uncountably many $\mathscr{U}$-minor-closed sets of functions. It also follows that not every $\mathscr{U}$-minor-closed set of functions is finitely generated, since if every $\mathscr{U}$-minor-closed set were generated by a finite set of generators drawn from the countably infinite set of Boolean functions, there would be only countably many $\mathscr{U}$-minor-closed sets. A corresponding construction for $\mathscr{I}$-minor-closed sets of functions is given by Ekin et al. [5].

Finally, we observe that the classification of the k-ean clones that are $\mathscr{Q}$-minor-closed has, for several choices of $\mathscr{Q}$, already been investigated. For a clone $\mathscr{F}$ is $\mathscr{Q}$-minor-closed if and only if $\mathscr{Q} \subseteq \mathscr{F}$. Thus the $\mathscr{U}$-minor-closed k-ean clones form a chain of length $k+1$, as has been shown by Burle [3]. Similar results for the cases in which $\mathscr{Q}$ comprises all permutations of $\mathbf{B}_k$, and where $\mathscr{Q}$ comprises all non-permutations (together with the identity function), are given by Haddad and Rosenberg [9,10] and Denham [4]. In all these cases, there are only finitely many clones that are $\mathscr{Q}$-minor-closed.

In the case where $\mathscr{Q}$ comprises just the constant functions (together with the identity function), there are 7 such clones if $k=2$ (see [20]), but uncountably many if $k \geqslant 3$ (see [1]).

4. Conclusion

We have constructed a Galois theory applicable to sets of finite functions that are closed under taking minors, in a broad sense of that term. This theory is not applicable, however, to sets that are not closed under diagonalization. Thus it cannot deal with sets of functions, such as the “unate functions” (see [15,7]) or the monotone Boolean functions corresponding to “binary clutters” (see [21]), that are closed under substituting constants for arguments, but not under identifying arguments. Hellerstein [11] has dealt with some of these classes by an extension of the theory presented in this paper.

Acknowledgements

The author would like to thank Lisa Hellerstein for sending a copy of the paper [5], which served as the starting point for the present work. He would also like to thank the three anonymous referees, who provided valuable and detailed comments on an earlier version of this paper.

Appendix. The equivalence of constraints and equations

For the purposes of this appendix, a *Boolean equation* has the form

$$P(f(E_1(x^1,\dots,x^q)),\dots,f(E_p(x^1,\dots,x^q))),$$

where P is a p-place Boolean predicate and $E_1,\dots,E_p$ are q-place Boolean expressions. If f is an n-adic Boolean function, the arguments $x^1=(x^1_1,\dots,x^1_n),\dots,x^q=(x^q_1,\dots,x^q_n)$ are interpreted as n-tuples of Boolean values, and all the Boolean operations in the expressions $E_1,\dots,E_p$ are interpreted as being applied componentwise to n-tuples of Boolean values to yield the p n-tuples of Boolean values to which the p occurrences of f are applied. The equation as a whole is *satisfied* by a function f if, whatever values are assigned to the arguments $x^1,\dots,x^q$, the resulting p values of the function f satisfy the predicate P.

Proposition A.1. *For every Boolean equation, there is a Boolean constraint that is satisfied by exactly the same set of functions.*

Proof. Let the p-ary relation R comprise the columns

$$\begin{pmatrix} E_1(x^1,\ldots,x^q) \\ \vdots \\ E_p(x^1,\ldots,x^q) \end{pmatrix},$$

where $x^1,\ldots,x^q$ range over all Boolean values. Let the p-ary relation S comprise the columns

$$\begin{pmatrix} y_1 \\ \vdots \\ y_p \end{pmatrix}$$

for which the Boolean values $y_1,\ldots,y_p$ satisfy the predicate P. Then the constraint (R,S) fulfills the conclusion of the proposition. □

Proposition A.2. *For every Boolean constraint, there is a Boolean equation that is satisfied by exactly the same set of functions.*

Proof. Let (R,S) be a p-ary constraint. If $R=\emptyset$, then (R,S) is satisfied by every Boolean function, and we may take the Boolean equation $f(x)=f(x)$, for example, to fulfill the conclusion of the proposition. Suppose, then, that the column

$$\begin{pmatrix} c_1 \\ \vdots \\ c_p \end{pmatrix}$$

belongs to R. Let Q be a p-place Boolean expression that is satisfied by the Boolean values $y_1,\ldots,y_p$ if and only if the column

$$\begin{pmatrix} y_1 \\ \vdots \\ y_p \end{pmatrix}$$

belongs to R. Let P be a p-place Boolean expression that is satisfied by the Boolean values $y_1,\ldots,y_p$ if and only if the column

$$\begin{pmatrix} y_1 \\ \vdots \\ y_p \end{pmatrix}$$

belongs to S. Then, taking $q=p$, the equation

$$P(f(E_1(x^1,\ldots,x^p)),\ldots,f(E_p(x^1,\ldots,x^p))),$$

where the expression $E_i(x^1,\ldots,x^p)$ is given by

$$(x^i \wedge Q(x^1,\ldots,x^p)) \vee (c_i \wedge \overline{Q(x^1,\ldots,x^p)}),$$

fulfills the conclusion of the proposition. □

References

[1] I. Ágoston, J. Demetrovics, L. Hannák, On the number of clones containing all constants, Colloq. Math. Soc. János Bolyai 43 (1983) 21–25.
[2] V.G. Bodnarchuk, L.A. Kaluzhnin, V.N. Kotov, B.A. Romov, Galois theory for Post algebras. I, II, Cybernetics 5 (1969) 243–252, 531–539.
[3] G.A. Burle, Classes of k-valued logic which contain all functions of a single variable, Discretnyĭ Analiz 10 (1967) 3–7.
[4] G.C. Denham, Many-valued generalizations of two finite intervals in Post's lattice, Proceedings of the International Symposium on Multi-Valued Logic, Vol. 24, 1994, pp. 314–318.
[5] O. Ekin, S. Foldes, P.L. Hammer, L. Hellerstein, Equational characterizations of Boolean function classes, Discrete Math. 211 (2000) 27–51.
[6] C.J. Everett, Closure operations and Galois theory in lattices, Trans. AMS 55 (1944) 514–525.
[7] A. Feigelson, L. Hellerstein, The forbidden projections of unate functions, Discrete Appl. Math. 77 (1997) 221–236.
[8] D. Geiger, Closed systems of functions and predicates, Pacific J. Math. 27 (1968) 95–100.
[9] L. Haddad, I.G. Rosenberg, A note on finite clones containing all permutations, Proceedings of the International Symposium on Multi-Valued Logic, Vol. 20, 1990, pp. 34–41.
[10] L. Haddad, I.G. Rosenberg, Finite clones containing all permutations, Can. J. Math. 46 (1994) 951–970.
[11] L. Hellerstein, On generalized constraints and certificates, Discrete Math. 226 (2001) 211–232.
[12] M. Krasner, Une generalisation de la notion de corps, J. Math. Pures Appl. 17 (1938) 367–385.
[13] M. Krasner, Abstract Galois theory and endotheory. I, Acta Sci. Math. 50 (1986) 253–286.
[14] M. Krasner, Abstract Galois theory and endotheory. II, Acta Sci. Math. 52 (1988) 231–255.
[15] R. McNaughton, Unate truth functions, IRE Trans. Electron. Comput. 10 (1961) 1–6.
[16] Ø. Ore, Galois connexions, Trans. AMS 55 (1944) 493–513.
[17] R. Pöschel, Postsche Algebren von Funktionen über einer Familie endlicher Mengen, Z. Math. Logik Grundl. Math. 19 (1973) 37–74.
[18] R. Pöschel, Die funktionale Vollständigkeit von Funktionenklassen über einer Familie endlicher Mengen, Z. Math. Logik Grundl. Math. 19 (1973) 37–74.
[19] R. Pöschel, L.A. Kaluzhnin, Funktionen- und Relationenalgebren, Birkhäuser, Basel, 1979.
[20] E. Post, The Two-Valued Iterative Systems of Mathematical Logic, Princeton University Press, Princeton, 1941.
[21] P.D. Seymour, The forbidden minors of binary clutters, J. London Math. Soc. 12 (2) (1976) 356–360.
[22] C. Wang, Boolean minors, Discrete Math. 141 (1995) 237–258.
[23] C. Wang, A.C. Williams, The threshold order of a Boolean function, Discrete Appl. Math. 31 (1991) 51–69.
[24] M. Ward, The closure operators of lattice, Ann. Math. 43 (1942) 191–196.
[25] R.O. Winder, Fundamentals of threshold logic, in: J.T. Tou (Ed.), Applied Automata Theory, Academic Press, New York, 1968, pp. 235–318.